

An explicit candidate for the set of Steinitz classes of tame Galois extensions with fixed Galois group of odd order

Luca Caputo and Alessandro Cobbe

March 6, 2012

ABSTRACT -Given a finite group G and a number field k , a well-known conjecture asserts that the set $R_t(k, G)$ of Steinitz classes of tame G -Galois extensions of k is a subgroup of the ideal class group of k . In this paper we investigate an explicit candidate for $R_t(k, G)$, when G is of *odd* order. More precisely, we define a subgroup $\mathcal{W}(k, G)$ of the class group of k and we prove that $R_t(k, G) \subseteq \mathcal{W}(k, G)$. We show that equality holds for all groups of odd order for which a description of $R_t(k, G)$ is known so far. Furthermore, by refining techniques introduced in [8], we use the Shafarevich-Weil Theorem in cohomological class field theory, to construct some tame Galois extensions with given Steinitz class. In particular, this allows us to prove the equality $R_t(k, G) = \mathcal{W}(k, G)$ when G is a group of order dividing ℓ^4 , where ℓ is an odd prime.

1 Introduction

Let K/k be an extension of number fields and let \mathcal{O}_K and \mathcal{O}_k be the rings of integers of K and k respectively. Then

$$\mathcal{O}_K \cong \mathcal{O}_k^{[K:k]-1} \oplus I$$

as \mathcal{O}_k -modules, where I is an ideal in \mathcal{O}_k which is determined by the extension K/k up to principal ideals. The ideal class of I is called the Steinitz class $\text{st}(K/k)$ of the extension.

For a number field k , denote by $\text{Cl}(k)$ the class group of k . If G is a finite group, one can consider the set of all Steinitz classes which arise from tame G -Galois extensions of k :

$$R_t(k, G) = \{x \in \text{Cl}(k) : \exists K/k \text{ tame Galois, } \text{Gal}(K/k) \cong G, \text{st}(K/k) = x\}.$$

There is no known description of $R_t(k, G)$ in general, but in all cases for which it is known it turns out to be a subgroup of the ideal class group of k . This leads to formulate the following conjecture.

Conjecture 1.1. For any number field k and any finite group G , $R_t(k, G)$ is a subgroup of $\text{Cl}(k)$.

The conjecture is known to hold for abelian groups as a consequence of the results of the paper [14] by Leon McCulloh. An explicit description of $R_t(k, G)$ for abelian

groups of odd order was first found by Lawrence Paul Endo in his unpublished PhD thesis [10], in which he also obtained some explicit results in the even case.

Concerning nonabelian groups, there are a lot of results for groups of some particular shape, however sometimes with restrictions on the base field k . A list of recent results includes [1], [2], [4], [5], [6], [7], [8], [9], [11], [12], [13], [18], [20], [21] and [22].

The aim of this paper is to develop some new ideas to improve the results of [8] and [9]. In Section 2 we generalize [8, Lemma 3.14], obtaining some limitations on the prime ideals which can ramify in tame Galois extensions of a number field with Galois group G . In particular, this gives an inclusion of $R_t(k, G)$ in an explicitly described subgroup of $\text{Cl}(k)$, which we baptize $\mathcal{W}(k, G)$ (see Definition 2.11). It seems natural to ask whether this inclusion is always an equality for groups of odd order (see Question 2.18), while some results contained in [10] give counterexamples already for abelian groups of even order. Note, in particular, that a positive answer to Question 2.18 would have Conjecture 1.1 as a consequence (for groups of odd order).

In Section 3 we extend the result of [8, Proposition 3.13], using a theorem by Shafarevich and Weil as a tool to construct Galois extensions of a given number field. The main idea is to use some cohomological information encoded in the reciprocity map of an abelian extension of a number field, which is itself a Galois extension of a smaller field.

In the last two sections we answer affirmatively to Question 2.18 for A' -groups of odd order (A' -groups have been introduced in [8], see also Definition 4.1) and for ℓ -groups of order up to ℓ^4 , where ℓ is an odd prime.

The case of groups of prime power order already shows some interesting complications, since for instance a two-step approach corresponding to a given splitting of the group as a semidirect product is not always enough to obtain all the needed Steinitz classes. The difficulty here comes from those extensions with prime ideals ramifying in both steps which, contrary to the case of A' -groups, cannot be left out. More precisely, given an *arbitrary* element $\tau \in G$, we need to exhibit tame G -Galois extensions such that τ is a generator of the inertia group of some prime ideals belonging to some prescribed ideal classes. To this aim, in Section 5, we develop a technique involving the construction of a larger Galois extension of the ground field, whose Galois group has G as a quotient (see the proof of Lemma 5.8). This method may be used to prove the equality $R_t(k, G) = \mathcal{W}(k, G)$ for a lot of other groups G of some particular kind. Anyway, we do not believe that it is worth to include more examples and we feel that one probably needs significantly new ideas to get some more general results.

2 Some necessary conditions for the ramification of prime ideals in tame Galois extensions

For the rest of the paper we will use the letter G to denote a finite group. For any $\tau \in G$, let $N_G(\tau)$ (resp. $C_G(\tau)$) be the normalizer (resp. the centralizer) of the subgroup of G generated by τ and let $o(\tau)$ be the order of τ . For a positive integer s , ζ_s will denote a primitive s -th root of unity. Finally we will always use the letter ℓ only for rational prime numbers, even if not explicitly indicated.

For any $\tau \in G$, we define a homomorphism

$$\varphi_\tau : N_G(\tau) \rightarrow (\mathbb{Z}/o(\tau)\mathbb{Z})^\times$$

by $\varphi_\tau(\sigma) = \alpha$, where $\sigma\tau\sigma^{-1} = \tau^\alpha$. Furthermore, if k is a number field, we need the cyclotomic character

$$\nu_{k,\tau} : \text{Gal}(k(\zeta_{o(\tau)})/k) \rightarrow (\mathbb{Z}/o(\tau)\mathbb{Z})^\times,$$

which is defined by $\nu_{k,\tau}(g) = \beta$, where $g(\zeta_{o(\tau)}) = \zeta_{o(\tau)}^\beta$. Note that $\nu_{k,\tau}$ is injective. We also set

$$H_{k,G,\tau} = \nu_{k,\tau}^{-1}(\varphi_\tau(N_G(\tau))) \subseteq \text{Gal}(k(\zeta_{o(\tau)})/k)$$

and we call $E_{k,G,\tau}$ the subfield of $k(\zeta_{o(\tau)})$ which is fixed by $H_{k,G,\tau}$.

Remark 2.1. We have the following commutative diagram

$$\begin{array}{ccc} \varphi_\tau^{-1}(\nu_{k,\tau}(\text{Gal}(k(\zeta_{o(\tau)})/k))) & \xrightarrow{\iota} & N_G(\tau) \\ \downarrow \nu_{k,\tau}^{-1} \circ \varphi_\tau & & \downarrow \varphi_\tau \\ \text{Gal}(k(\zeta_{o(\tau)})/k) & \xrightarrow{\nu_{k,\tau}} & (\mathbb{Z}/o(\tau)\mathbb{Z})^\times \end{array}$$

and it is easy to verify that $\varphi_\tau^{-1}(\nu_{k,\tau}(\text{Gal}(k(\zeta_{o(\tau)})/k)))$ is the pullback of φ_τ and $\nu_{k,\tau}$. Its image in $\text{Gal}(k(\zeta_{o(\tau)})/k)$ is exactly $H_{k,G,\tau}$.

We start proving some elementary properties of the number fields $E_{k,G,\tau}$, which will be useful throughout the paper.

Lemma 2.2. *Suppose that $G = H \rtimes_\mu \mathcal{G}$ is the (internal) semidirect product of two subgroups, H and \mathcal{G} . Then, for all $\sigma \in \mathcal{G}$, we have*

$$E_{k,G,\sigma} = E_{k,\mathcal{G},\sigma}.$$

If H is abelian, then, for all $\tau \in H$, $E_{k,G,\tau}$ coincides with the $E_{k,\mu,\tau}$ defined in [8, Section 3.1].

Proof. Let $\sigma \in \mathcal{G}$ and let $\sigma_1 \in \mathcal{G}$, $\tau_1 \in H$ be such that $\sigma_1\tau_1 \in N_G(\sigma)$. Then

$$\sigma^{\varphi_\sigma(\sigma_1\tau_1)} = \sigma_1\tau_1\sigma\tau_1^{-1}\sigma_1^{-1} = (\sigma_1\tau_1\sigma_1^{-1})(\sigma_1\sigma\tau_1^{-1}\sigma^{-1}\sigma_1^{-1})\sigma_1\sigma\sigma_1^{-1}.$$

Since $\sigma_1\tau_1\sigma_1^{-1}$, $\sigma_1\sigma\tau_1^{-1}\sigma^{-1}\sigma_1^{-1} \in H$ and each element of G can be written uniquely as a product of an element of H and one of \mathcal{G} , we deduce that

$$(\sigma_1\tau_1\sigma_1^{-1})(\sigma_1\sigma\tau_1^{-1}\sigma^{-1}\sigma_1^{-1}) = 1$$

and

$$\sigma^{\varphi_\sigma(\sigma_1\tau_1)} = \sigma_1\sigma\sigma_1^{-1}.$$

Hence $\sigma_1 \in N_{\mathcal{G}}(\sigma)$ and $\varphi_\sigma(\sigma_1\tau_1) = \varphi_\sigma(\sigma_1)$. Therefore we obtain

$$\varphi_\sigma(N_G(\sigma)) = \varphi_\sigma(N_{\mathcal{G}}(\sigma)),$$

i.e.

$$E_{k,G,\sigma} = E_{k,\mathcal{G},\sigma}.$$

The second part of the lemma is trivial. □

Lemma 2.3. *Let $\sigma \in G$ and $n \in \mathbb{N}$. Then*

$$E_{k,G,\sigma^n} \subseteq E_{k,G,\sigma}.$$

In particular if $\tau \in G$ generates the same cyclic subgroup as σ , then

$$E_{k,G,\sigma} = E_{k,G,\tau}.$$

Proof. We consider the restriction

$$\text{res} : \text{Gal}(k(\zeta_{o(\sigma)})/k) \rightarrow \text{Gal}(k(\zeta_{o(\sigma^n)})/k)$$

and the projection

$$\pi : (\mathbb{Z}/o(\sigma)\mathbb{Z})^\times \rightarrow (\mathbb{Z}/o(\sigma^n)\mathbb{Z})^\times.$$

Using that $N_G(\sigma) \subseteq N_G(\sigma^n)$, we get commutative diagrams

$$\begin{array}{ccc} N_G(\sigma) & \xrightarrow{\varphi_\sigma} & (\mathbb{Z}/o(\sigma)\mathbb{Z})^\times \\ \downarrow \iota & & \downarrow \pi \\ N_G(\sigma^n) & \xrightarrow{\varphi_{\sigma^n}} & (\mathbb{Z}/o(\sigma^n)\mathbb{Z})^\times \end{array} \quad \begin{array}{ccc} \text{Gal}(k(\zeta_{o(\sigma)})/k) & \xrightarrow{\nu_{k,\sigma}} & (\mathbb{Z}/o(\sigma)\mathbb{Z})^\times \\ \downarrow \text{res} & & \downarrow \pi \\ \text{Gal}(k(\zeta_{o(\sigma^n)})/k) & \xrightarrow{\nu_{k,\sigma^n}} & (\mathbb{Z}/o(\sigma^n)\mathbb{Z})^\times. \end{array}$$

Therefore $H_{k,G,\sigma} \subseteq \text{res}^{-1}(H_{k,G,\sigma^n})$, since

$$\begin{aligned} H_{k,G,\sigma} &= \nu_{k,\sigma}^{-1}(\varphi_\sigma(N_G(\sigma))) \\ &\subseteq \text{res}^{-1}(\nu_{k,\sigma^n}^{-1}(\nu_{k,\sigma^n}(\text{res}(\nu_{k,\sigma}^{-1}(\varphi_\sigma(N_G(\sigma))))) \\ &= \text{res}^{-1}(\nu_{k,\sigma^n}^{-1}(\pi(\nu_{k,\sigma}(\nu_{k,\sigma}^{-1}(\varphi_\sigma(N_G(\sigma))))) \\ &\subseteq \text{res}^{-1}(\nu_{k,\sigma^n}^{-1}(\pi(\varphi_\sigma(N_G(\sigma)))) \\ &= \text{res}^{-1}(\nu_{k,\sigma^n}^{-1}(\varphi_{\sigma^n}(\iota(N_G(\sigma)))) \\ &\subseteq \text{res}^{-1}(\nu_{k,\sigma^n}^{-1}(\varphi_{\sigma^n}(N_G(\sigma^n))) = \text{res}^{-1}(H_{k,G,\sigma^n}). \end{aligned}$$

Now the fixed field of $\text{res}^{-1}(H_{k,G,\sigma^n})$ in $k(\zeta_{o(\sigma)})$ coincides with the fixed field of H_{k,G,σ^n} in $k(\zeta_{o(\sigma^n)})$, i.e. with E_{k,G,σ^n} . Therefore

$$E_{k,G,\sigma^n} \subseteq E_{k,G,\sigma}.$$

□

Lemma 2.4. *Let $\sigma, \tau \in G$, then*

$$E_{k,G,\sigma} = E_{k,G,\tau\sigma\tau^{-1}}.$$

Proof. We observe that $N_G(\tau\sigma\tau^{-1}) = \tau N_G(\sigma)\tau^{-1}$. Further, for any $\rho \in N_G(\sigma)$, we have

$$\begin{aligned} (\tau\sigma\tau^{-1})^{\varphi_{\tau\sigma\tau^{-1}}(\tau\rho\tau^{-1})} &= (\tau\rho\tau^{-1})(\tau\sigma\tau^{-1})(\tau\rho\tau^{-1})^{-1} \\ &= \tau\rho\sigma\rho^{-1}\tau^{-1} = \tau\sigma^{\varphi_\sigma(\rho)}\tau^{-1} = (\tau\sigma\tau^{-1})^{\varphi_\sigma(\rho)}, \end{aligned}$$

i.e.

$$\varphi_{\tau\sigma\tau^{-1}}(\tau\rho\tau^{-1}) = \varphi_\sigma(\rho).$$

Therefore

$$\varphi_{\tau\sigma\tau^{-1}}(N_G(\tau\sigma\tau^{-1})) = \varphi_{\tau\sigma\tau^{-1}}(\tau N_G(\sigma)\tau^{-1}) = \varphi_\sigma(N_G(\sigma))$$

and, since clearly $\nu_{k,\sigma} = \nu_{k,\tau\sigma\tau^{-1}}$, we conclude that $H_{k,G,\sigma} = H_{k,G,\tau\sigma\tau^{-1}}$, and therefore $E_{k,G,\sigma} = E_{k,G,\tau\sigma\tau^{-1}}$. □

We recall the following important definition from [10, Section I.2] (see also [8, Definition 2.8 and Proposition 2.10]).

Definition 2.5. For any finite abelian extension K/k of number fields, we define

$$W(k, K) = N_{K/k} J_K \cdot P_k / P_k \subseteq \text{Cl}(k),$$

where J_K is the group of fractional ideals of K , P_k is the group of principal ideals in k and the map $N_{K/k}$ is induced by the norm from K to k . For any positive integer m , we use the notation $W(k, m) = W(k, k(\zeta_m))$.

The following lemma is an immediate consequence of the definition.

Lemma 2.6. Let $L \supseteq K \supseteq k$ be number fields. Then

$$W(k, L) \subseteq W(k, K).$$

Proof. Actually: $N_{L/k} J_L = N_{K/k}(N_{L/K} J_L) \subseteq N_{K/k} J_K$. □

For an integer n and a prime number ℓ , we will always indicate by $n(\ell)$ the greatest power of ℓ dividing n . For an element $\sigma \in G$ of order $o(\sigma)$, we will denote by $\sigma(\ell)$ the element $\sigma^{o(\sigma)/o(\sigma)(\ell)}$, which is of order $o(\sigma)(\ell)$. Further we will denote by $G\{\ell\}$ the set of all the elements $\sigma \in G$ such that $\sigma(\ell) = \sigma$, i.e. of all the elements of order a power of ℓ .

Let A be a subgroup of an abelian group B (written multiplicatively). For $t \in \frac{1}{2}\mathbb{N} \subset \mathbb{Q}$, we set

$$A_B^t = \begin{cases} \{x \in A : \exists a \in A, x = a^t\} & \text{if } t \in \mathbb{N} \\ \{x \in B : \exists a \in A, x^2 = a^{2t}\} & \text{if } t \notin \mathbb{N}. \end{cases}$$

In the above notation, we shall always omit the index B , since it will be clear from the context (actually B will be an ideal class group).

We explicitly remark that in general $A \neq (A^2)^{1/2}$. For example, if A is the trivial subgroup of the group B with 2 elements, then $(A^2)^{1/2} = B \neq A$.

Lemma 2.7. Let m, n be positive integers. If every prime q dividing n also divides m , then $W(k, m)^n \subseteq W(k, mn)$.

Proof. By the assumptions on m and n , we have that

$$[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}(\zeta_m)] = \frac{\phi(mn)}{\phi(m)} = n,$$

and this is a multiple of $[k(\zeta_{mn}) : k(\zeta_m)]$. Now, for any $x \in W(k, m)$, there exists an ideal I in $k(\zeta_m)$ such that $N_{k(\zeta_m)/k} I$ is in the class of x . Hence we can conclude that $x^n \in W(k, mn)$, since

$$(N_{k(\zeta_m)/k} I)^n = N_{k(\zeta_{mn})/k} (I^{n/[k(\zeta_{mn}) : k(\zeta_m)]} \mathcal{O}_{k(\zeta_{mn})}).$$

The inclusion $W(k, m)^n \subseteq W(k, mn)$ follows. □

Lemma 2.8. Let A be a subgroup of an abelian group B . If $d|m$, then $A^{m/2} \subseteq A^{d/2}$.

Proof. Let $x \in A^{m/2}$. If d is even, then also m must be even, and it is clear that $x \in A^{d/2}$. If d is odd, then $x^2 \in A^m \subseteq A^d$, i.e. $x \in A^{d/2}$. \square

Lemma 2.9. *Let A be a subgroup of an abelian group B , let m_1, \dots, m_n be positive integers and let d be their greatest common divisor. Then*

$$\prod_{i=1}^n A^{m_i/2} = A^{d/2}.$$

Proof. \subseteq By Lemma 2.8, we have $A^{m_i/2} \subseteq A^{d/2}$ for $i = 1, \dots, n$.

\supseteq Let $x \in A^{d/2}$ and let $c_1, \dots, c_n \in \mathbb{Z}$ be such that $\sum_{i=1}^n c_i m_i = d$. If d is even, then also every m_i is even, and there exists $a \in A$ such that

$$x = a^{d/2} = a^{\sum_{i=1}^n c_i m_i/2} = \prod_{i=1}^n (a^{c_i})^{m_i/2} \in \prod_{i=1}^n A^{m_i/2}.$$

If d is odd, then there exists $a \in A$ such that $x^2 = a^d$. Now let $i \in \{1, \dots, n\}$. If m_i is odd, then

$$(x^{c_i m_i/d})^2 = a^{d(c_i m_i/d)} = a^{c_i m_i},$$

i.e.

$$x^{c_i m_i/d} \in A^{m_i/2}.$$

If m_i is even, then

$$x^{c_i m_i/d} = x^{2c_i m_i/(2d)} = a^{dc_i m_i/(2d)} = a^{c_i m_i/2} \in A^{m_i/2}.$$

Hence

$$x = x^{\sum_{i=1}^n c_i m_i/d} = \prod_{i=1}^n x^{c_i m_i/d} \in \prod_{i=1}^n A^{m_i/2}.$$

\square

If G is a group and S is a subset of G containing 1, we use the notation S^* for the subset $S \setminus \{1\}$.

Proposition 2.10. *Let k be a number field and let G be a finite group. Then, for $i = 0$ or 1, we have*

$$\prod_{\tau \in G^*} W(k, E_{k,G,\tau})^{\frac{o(\tau)-1}{2^i} \frac{\#G}{o(\tau)}} = \prod_{\ell \mid \#G} \prod_{\sigma \in G\{\ell\}^*} W(k, E_{k,G,\sigma})^{\frac{\ell-1}{2^i} \frac{\#G}{o(\sigma)}}.$$

Proof. \subseteq Using [8, Lemma 3.16], Lemma 2.8 and Lemma 2.9 (for the first inclusion in the following formula), Lemma 2.3 and Lemma 2.6 (for the second inclusion in the following formula), we see that

$$\begin{aligned} W(k, E_{k,G,\tau})^{\frac{o(\tau)-1}{2^i} \frac{\#G}{o(\tau)}} &\subseteq \prod_{\ell \mid o(\tau)} W(k, E_{k,G,\tau})^{\frac{\ell-1}{2^i} \frac{\#G}{o(\tau)(\ell)}} \\ &\subseteq \prod_{\ell \mid o(\tau)} W(k, E_{k,G,\tau(\ell)})^{\frac{\ell-1}{2^i} \frac{\#G}{o(\tau(\ell))}} \\ &\subseteq \prod_{\ell \mid \#G} \prod_{\sigma \in G\{\ell\}^*} W(k, E_{k,G,\sigma})^{\frac{\ell-1}{2^i} \frac{\#G}{o(\sigma)}}. \end{aligned}$$

\supseteq Let $\sigma \in G\{\ell\}^*$, where ℓ is a prime number dividing $\#G$, and set $\tilde{\sigma} = \sigma^{o(\sigma)/\ell}$. Clearly

$$\gcd\left((\ell-1)\frac{\#G}{\ell}, (o(\sigma)-1)\frac{\#G}{o(\sigma)}\right) = (\ell-1)\frac{\#G}{o(\sigma)}. \quad (1)$$

Hence, using Lemma 2.3, Lemma 2.6 and Lemma 2.9,

$$\begin{aligned} W(k, E_{k,G,\sigma})^{\frac{\ell-1}{2^i} \frac{\#G}{o(\sigma)}} &= W(k, E_{k,G,\sigma})^{\frac{\ell-1}{2^i} \frac{\#G}{\ell}} W(k, E_{k,G,\sigma})^{\frac{o(\sigma)-1}{2^i} \frac{\#G}{o(\sigma)}} \\ &\subseteq W(k, E_{k,G,\tilde{\sigma}})^{\frac{o(\tilde{\sigma})-1}{2^i} \frac{\#G}{o(\tilde{\sigma})}} W(k, E_{k,G,\sigma})^{\frac{o(\sigma)-1}{2^i} \frac{\#G}{o(\sigma)}} \\ &\subseteq \prod_{\tau \in G^*} W(k, E_{k,G,\tau})^{\frac{o(\tau)-1}{2^i} \frac{\#G}{o(\tau)}}. \end{aligned}$$

□

Definition 2.11. Let k be a number field and G be a finite group. Then we set

$$\mathcal{W}(k, G) = \prod_{\tau \in G^*} W(k, E_{k,G,\tau})^{\frac{o(\tau)-1}{2} \frac{\#G}{o(\tau)}} = \prod_{\ell | \#G} \prod_{\sigma \in G\{\ell\}^*} W(k, E_{k,G,\sigma})^{\frac{\ell-1}{2} \frac{\#G}{o(\sigma)}} \subseteq \text{Cl}(k).$$

We now come to the principal results of this section. We shall show that the classes of primes ramifying in a tame G -Galois extension of k have to satisfy some conditions. As a consequence, we will get the inclusion $R_t(k, G) \subseteq \mathcal{W}(k, G)$.

If K/k is a Galois extension of number fields and \mathfrak{P} is a prime ideal in K , we denote by $D(K/k, \mathfrak{P})$ (resp. $I(K/k, \mathfrak{P})$) the decomposition group (resp. the inertia group) of \mathfrak{P} in K/k . Further we denote by $d(K/k)$ the discriminant of K over k .

Proposition 2.12. *Let K/k be a tame G -Galois extension of number fields, let \mathfrak{p} be a prime of k ramifying in K/k and let τ be a generator of $I(K/k, \mathfrak{P})$, where \mathfrak{P} is a prime of K dividing \mathfrak{p} . Then*

$$x \in W(k, E_{k,G,\tau}),$$

where x is the class of \mathfrak{p} in $\text{Cl}(k)$.

Proof. Let $\tilde{\mathfrak{P}}$ be a prime above \mathfrak{P} in $K(\zeta_{o(\tau)})$. In order to show that $x \in W(k, E_{k,G,\tau})$, we will prove that $D(K(\zeta_{o(\tau)})/k, \tilde{\mathfrak{P}})$ is contained in $\text{Gal}(K(\zeta_{o(\tau)})/E_{k,G,\tau})$. It will follow that \mathfrak{p} has inertia degree 1 in $E_{k,G,\tau}/k$, and hence that it is the norm of an ideal in $E_{k,G,\tau}/k$.

Recall that there is a canonical isomorphism between $I(K/k, \mathfrak{P})$ and a subgroup of the units of the residue field $\kappa_{\mathfrak{P}}$ of K at \mathfrak{P} , which is easily seen to be invariant with respect to the action of the decomposition group of \mathfrak{P} in K/k (see [19, Proposition IV.2.7]). Hence $\kappa_{\mathfrak{P}}^\times$ contains an element of order $o(\tau)$ and therefore $\kappa_{\mathfrak{P}} = \kappa_{\tilde{\mathfrak{P}}}$, where the latter denotes the residue field of $K(\zeta_{o(\tau)})$ at $\tilde{\mathfrak{P}}$.

Let now $\delta \in D(K(\zeta_{o(\tau)})/k, \tilde{\mathfrak{P}})$. Then $\delta|_K \in N_G(\tau)$, since $\delta|_K \in D(K/k, \mathfrak{P})$ and $I(K/k, \mathfrak{P}) \triangleleft D(K/k, \mathfrak{P})$. By definition,

$$\tau^{\varphi_\tau(\delta|_K)} = (\delta|_K) \tau (\delta|_K)^{-1}$$

and therefore, using the invariance of the above mentioned isomorphism, $\delta|_K$ (and hence also δ) acts as raising to the power $\varphi_\tau(\delta|_K)$ on the subgroup of order $o(\tau)$ of

$\kappa_{\tilde{\mathfrak{P}}}^\times = \kappa_{\tilde{\mathfrak{P}}}^\times$. Recalling that the powers of $\zeta_{o(\tau)}$ are distinct modulo $\tilde{\mathfrak{P}}$ (since $\tilde{\mathfrak{P}} \nmid o(\tau)$), we get that

$$\zeta_{o(\tau)}^{\nu_{k,\tau}(\delta|_{k(\zeta_{o(\tau)})})} = \delta(\zeta_{o(\tau)}) = \zeta_{o(\tau)}^{\varphi_\tau(\delta|_K)}.$$

In particular, $\nu_{k,\tau}(\delta|_{k(\zeta_{o(\tau)})}) = \varphi_\tau(\delta|_K)$, i.e.

$$\delta|_{k(\zeta_{o(\tau)})} \in H_{k,G,\tau} = \text{Gal}(k(\zeta_{o(\tau)})/E_{k,G,\tau}).$$

Thus

$$\delta \in \text{Gal}(K(\zeta_{o(\tau)})/E_{k,G,\tau})$$

and, since the choice of $\delta \in D(K(\zeta_{o(\tau)})/k, \tilde{\mathfrak{P}})$ was arbitrary, we have

$$D(K(\zeta_{o(\tau)})/k, \tilde{\mathfrak{P}}) \subseteq \text{Gal}(K(\zeta_{o(\tau)})/E_{k,G,\tau}).$$

This shows that $x \in W(k, E_{k,G,\tau})$. □

Theorem 2.13. *Let k be a number field and G a finite group. Then*

$$\text{R}_t(k, G) \subseteq \mathcal{W}(k, G).$$

Proof. Let K/k be a tame Galois extension with Galois group G . Its discriminant is

$$d(K/k) = \prod_{\mathfrak{p}} \mathfrak{p}^{(e_{\mathfrak{p}}-1) \frac{\#G}{e_{\mathfrak{p}}}},$$

where the product runs over the primes \mathfrak{p} of k which ramify in K/k and whose ramification index in K/k is denoted by $e_{\mathfrak{p}}$. Note that $e_{\mathfrak{p}}$ equals the order of an element τ generating the inertia group of a prime ideal \mathfrak{P} of K dividing \mathfrak{p} .

If G has odd order or noncyclic 2-Sylow subgroups, then $d(K/k)$ is the square of an ideal whose class is $\text{st}(K/k)$, by [8, Theorem 2.1]. Hence, in this case, using Proposition 2.12 we obtain

$$\text{st}(K/k) \in \prod_{\tau \in G^*} W(k, E_{k,G,\tau})^{\frac{o(\tau)-1}{2} \frac{\#G}{o(\tau)}} = \mathcal{W}(k, G).$$

If G has nontrivial cyclic 2-Sylow subgroups, then by [8, Theorem 2.1] and Proposition 2.12 we only obtain

$$\text{st}(K/k) \in \left(\prod_{\tau \in G^*} W(k, E_{k,G,\tau})^{(o(\tau)-1) \frac{\#G}{o(\tau)}} \right)^{1/2}$$

i.e., using Proposition 2.10,

$$\text{st}(K/k)^2 \in \prod_{\ell \mid \#G} \prod_{\sigma \in G\{\ell\}^*} W(k, E_{k,G,\sigma})^{(\ell-1) \frac{\#G}{o(\sigma)}}.$$

This means that, for every $\ell \mid \#G$ and every $\sigma \in G\{\ell\}^*$, there exists $x_\sigma \in W(k, E_{k,G,\sigma})$ such that

$$\text{st}(K/k)^2 = \prod_{\ell \mid \#G} \prod_{\sigma \in G\{\ell\}^*} x_\sigma^{(\ell-1) \frac{\#G}{o(\sigma)}}.$$

In the above formula, the only odd exponents in the right-hand side are those corresponding to the elements $\sigma \in G$ of order $\#G(2)$ (see the notation after Lemma 2.6). For all the other terms we have

$$\prod_{\ell \mid \#G} \prod_{\substack{\sigma \in G\{\ell\}^* \\ o(\sigma) \neq \#G(2)}} x_\sigma^{\frac{\ell-1}{2} \frac{\#G}{o(\sigma)}} \in \prod_{\ell \mid \#G} \prod_{\sigma \in G\{\ell\}^*} W(k, E_{k,G,\sigma})^{\frac{\ell-1}{2} \frac{\#G}{o(\sigma)}}.$$

Further

$$\left(\text{st}(K/k) \prod_{\ell \mid \#G} \prod_{\substack{\sigma \in G\{\ell\}^* \\ o(\sigma) \neq \#G(2)}} x_\sigma^{-\frac{\ell-1}{2} \frac{\#G}{o(\sigma)}} \right)^2 \in \prod_{\sigma \in G: o(\sigma) = \#G(2)} W(k, E_{k,G,\sigma})^{\frac{\#G}{o(\sigma)}}.$$

By the Sylow Theorems, all the 2-Sylow subgroups of G are conjugate to a single cyclic group, generated, say, by an element $\tilde{\sigma}$. Hence, for every $\sigma \in G$ of order $\#G(2)$, there exists $\tau \in G$ such that $\langle \sigma \rangle = \langle \tau \tilde{\sigma} \tau^{-1} \rangle$. Therefore, by Lemma 2.4 and Lemma 2.3, for all such σ , $E_{k,G,\sigma} = E_{k,G,\tilde{\sigma}}$. So we obtain

$$\text{st}(K/k) \prod_{\ell \mid \#G} \prod_{\substack{\sigma \in G\{\ell\}^* \\ o(\sigma) \neq \#G(2)}} x_\sigma^{-\frac{\ell-1}{2} \frac{\#G}{o(\sigma)}} \in W(k, E_{k,G,\tilde{\sigma}})^{\frac{1}{2} \frac{\#G}{o(\sigma)}}.$$

i.e.

$$\text{st}(K/k) \in \prod_{\ell \mid \#G} \prod_{\sigma \in G\{\ell\}^*} W(k, E_{k,G,\sigma})^{\frac{\ell-1}{2} \frac{\#G}{o(\sigma)}} = \mathcal{W}(k, G).$$

This completes the proof. \square

Remark 2.14. Using the results of L. McCulloh on realizable classes, one can obtain a different proof of Theorem 2.13. More precisely for a tame G -Galois extension K/k , let $\text{cl}_{\mathcal{O}_k[G]}(\mathcal{O}_K)$ denote the class defined by \mathcal{O}_K in the projective class group $\text{Cl}(\mathcal{O}_k[G])$. Then McCulloh proved that, for every number field k and every group G , the set

$$R(\mathcal{O}_k[G]) = \{\xi \in \text{Cl}(\mathcal{O}_k[G]) : \exists K/k \text{ tame Galois, } \text{Gal}(K/k) \cong G, \text{cl}_{\mathcal{O}_k[G]}(\mathcal{O}_K) = \xi\}$$

is contained in the kernel of a homomorphism defined on $\text{Cl}(\mathcal{O}_k[G])$ (see [15]). He then used this inclusion to derive an equivalent version of Theorem 2.13 (see [16]).

One may wonder for which groups the inclusion of the above theorem is actually an equality (for every number field k). It is easy to find groups of even order for which the inclusion may be strict for some number fields.

Example 2.15. Let $k = \mathbb{Q}(i, \sqrt{10})$ and $G = C(8)$ be a cyclic group of order 8. The field $k(\zeta_8)$ is obtained extending k with a root of the polynomial $x^2 - i$, whose roots are ζ_8 and ζ_8^5 . Hence

$$\text{Gal}(k(\zeta_8)/k) \subseteq \text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) = (\mathbb{Z}/8\mathbb{Z})^\times$$

is of order 2 and is generated by the class of 5. In particular it is different from the subgroups generated by the class of -5 and by the class of -25 . We obtain by [10, II.2.6] that

$$R_t(k, C(8)) = W(k, 8).$$

On the other hand, it is easy to verify, using Lemma 2.7, that $\mathcal{W}(k, C(8)) = W(k, 8)^{\frac{1}{2}}$. We now show that $R_t(k, C(8)) \neq \mathcal{W}(k, C(8))$. Actually, an easy calculation with PARI/GP shows that $\text{Cl}(k(\zeta_8))$ is trivial, while $\text{Cl}(k)$ is of order 2. It follows that $R_t(k, C(8)) = W(k, 8)$ is the trivial group, while $\mathcal{W}(k, C(8)) = W(k, 8)^{\frac{1}{2}}$ is equal to $\text{Cl}(k)$, which is of order 2. \square

On the other hand, for a lot of groups of odd order, including those for which Conjecture 1.1 is known to hold so far, we will show in Sections 4 and 5 that the inclusion of Theorem 2.13 is indeed an equality (for every number field k). To simplify statements in the next sections, we will adopt the following working definitions.

Definition 2.16. Given a number field F , we will say that an extension K/k of number fields satisfies the property $P(F)$ if it is tame, with no nontrivial unramified subextensions and such that $d(K/k)$ is prime to $d(F/\mathbb{Q})$. To simplify notations we will say that K/k satisfies $P(s)$ if it satisfies $P(k(\zeta_s))$.

Definition 2.17. We call a finite group G *very good* if the following conditions hold:

1. For every number field k , we have

$$R_t(k, G) = \mathcal{W}(k, G).$$

2. For every number field k , for every class $x \in R_t(k, G)$ and every positive integer s , there exists a G -Galois extension K/k with Steinitz class x and satisfying $P(s)$.

It is clear that a very good group of odd order is also good, in the sense of [8, Definition 3.15]. Further it seems reasonable to expect that the second condition of the above definition is satisfied for every group G , including those not satisfying the first condition.

With these definitions and in view of the results that will be proved in Sections 4 and 5, it seems natural to ask the following question.

Question 2.18. Is every group G of odd order very good?

Of course a positive answer would also imply Conjecture 1.1 for all groups of odd order.

We do not know the answer to Question 2.18, but we suspect that it might be affirmative. The main point here is to construct tame G -Galois extensions with some given Steinitz classes; of course this could be very difficult in general, but in the next section we will give some results in this direction.

3 Constructive inclusion

In this section we develop some techniques, which we will need in the last two sections to construct some tame Galois extensions of number fields with given Galois groups and Steinitz classes.

Let \mathcal{G} be a finite group and let H be an abelian group. Let $\mu : \mathcal{G} \rightarrow \text{Aut}(H)$ be an action of \mathcal{G} on H and let G be a group such that there exists an exact sequence

$$1 \rightarrow H \rightarrow G \rightarrow \mathcal{G} \rightarrow 1 \tag{2}$$

and the action of \mathcal{G} on H induced by the conjugation coincides with μ . Let k_1 be a \mathcal{G} -Galois extension of a number field k and K/k_1 an H -Galois extension such that K/k is Galois with Galois group G . Let C_{k_1} be the idèle class group of k_1 .

Theorem 3.1 (Shafarevich-Weil). *With notation and hypotheses as above, the reciprocity map $(\cdot, K/k_1) : C_{k_1} \rightarrow H$ induces a map*

$$H^2(\mathcal{G}, C_{k_1}) \rightarrow H^2(\mathcal{G}, H),$$

which sends the fundamental class $u \in H^2(\mathcal{G}, C_{k_1})$ to the class of the group extension (2). In particular, the image of u is trivial precisely when G is isomorphic to the semidirect product $H \rtimes_{\mu} \mathcal{G}$.

Proof. See [17, Theorem 2.110]. □

Using Theorem 3.1 we can improve the result of [8, Proposition 3.13]. In that paper, the action μ was assumed to be such that $H^2(\mathcal{G}, H)$ is trivial. This assumption is satisfied in some particular cases (for example when the orders of H and \mathcal{G} are coprime, by a theorem of Schur-Zassenhaus), but of course not in general. We are going to use Theorem 3.1 to study groups G of the form $H \rtimes_{\mu} \mathcal{G}$, where $H^2(\mathcal{G}, H)$ is no more assumed to be trivial. The proof will work exactly as in [8], except for some details, which are pointed out in what follows; for the unchanged parts we will refer the reader to [8].

From now on, in this section, G will be of the form $H \rtimes_{\mu} \mathcal{G}$, where H is an abelian group of *odd* order.

Lemma 3.2. *Let s be a positive integer and let k_1 be a tame \mathcal{G} -Galois extension of k satisfying $P(s)$. Then there exists a tame H -Galois extension K of k_1 , such that K/k is G -Galois and satisfying the following conditions.*

1. *The prime ideals ramifying in K/k_1 are principal.*
2. *$\text{st}(K/k_1) = 1$.*
3. *K/k_1 satisfies $P(s)$.*

Proof. Choose a set $\{\mathfrak{P}_1, \dots, \mathfrak{P}_t\}$ of prime ideals in k_1 which are unramified over \mathbb{Q} and whose classes generate $\text{Cl}(k_1)$. Now recall the definition of the so-called content map:

$$\pi : I_{k_1} \rightarrow J_{k_1}, \quad \alpha \mapsto \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})},$$

where I_{k_1} and J_{k_1} are the idèle group and the ideal group of k_1 , respectively. For every $i \in \{1, \dots, t\}$, let $\pi_{\mathfrak{P}_i}$ be a prime element in the completion $(k_1)_{\mathfrak{P}_i}$ and let y_i be the idèle in I_{k_1} whose component at \mathfrak{P}_i (resp. at any prime different from \mathfrak{P}_i) is $\pi_{\mathfrak{P}_i}$ (resp. 1).

Let $\tilde{u} : \mathcal{G} \times \mathcal{G} \rightarrow C_{k_1}$ be a cocycle, whose class in $H^2(\mathcal{G}, C_{k_1})$ is the fundamental class u . Recall that we have an exact sequence

$$1 \rightarrow \prod_{\mathfrak{P}} U_{\mathfrak{P}}/U_{k_1} \rightarrow C_{k_1} \xrightarrow{\pi} \text{Cl}(k_1) \rightarrow 1,$$

where U_{k_1} is the group of units of k_1 and $\prod_{\mathfrak{p}} U_{\mathfrak{p}} \subseteq I_{k_1}$ is the group of unit idèles. Therefore, for all couples $(\rho_1, \rho_2) \in \mathcal{G} \times \mathcal{G}$, we can find $v_{\rho_1, \rho_2} \in \prod_{\mathfrak{p}} U_{\mathfrak{p}}$ and $\lambda_{\rho_1, \rho_2, j} \in \mathbb{Z}$ such that $\tilde{u}(\rho_1, \rho_2)$ is represented by $v_{\rho_1, \rho_2} \prod_{j=1}^t y_j^{\lambda_{\rho_1, \rho_2, j}}$.

We add all the elements v_{ρ_1, ρ_2} to the set $\{u_1, \dots, u_T\}$ defined in [8], before Lemma 3.9. The arguments of [8, Lemma 3.10], with $x = 1$, give a tame H -Galois extension K of k_1 , which is also Galois over k , and such that the action of \mathcal{G} on H induced by the conjugation is μ . Further, by construction, the kernel of the reciprocity map $(\cdot, K/k_1) : C_{k_1} \rightarrow \text{Gal}(K/k_1) = H$ contains all the elements $\tilde{u}(\rho_1, \rho_2)$ with $\rho_1, \rho_2 \in \mathcal{G}$. Therefore the image of the fundamental class by the reciprocity map corresponding to the extension K/k_1 must be trivial and so, by Theorem 3.1, the Galois group of K/k must be isomorphic to $H \rtimes_{\mu} \mathcal{G}$.

Finally, the construction of the proof of [8, Lemma 3.10] implies that the primes $\mathfrak{q}_1, \dots, \mathfrak{q}_{r+1}$ of k_1 ramifying in K/k_1 are in the class of $x = 1$, hence principal. Since H is of odd order, we deduce that $\text{st}(K/k_1) = 1$, i.e. we have proved conditions 1 and 2. As for condition 3, it follows, once more by the proof of [8, Lemma 3.10], that K/k_1 has no nontrivial unramified subextensions and that the \mathfrak{q}_i can be chosen so that their restrictions to \mathbb{Q} are unramified in $k_1(\zeta_s)/\mathbb{Q}$. \square

Lemma 3.3. *Let s be a multiple of $\#H$ and let k_1 be a tame \mathcal{G} -Galois extension of k satisfying $P(s)$. For every prime number ℓ dividing $\#H$ and every $\tau \in H\{\ell\}^*$, let x_{τ} be any class in $W(k, E_{k, G, \tau})$ and let A_{τ}, B_{τ} be nonnegative integers, with $A_{\tau} \neq 1$. Then there exists a tame H -Galois extension K of k_1 , such that K/k is G -Galois and satisfying the following conditions.*

1. *The only nonprincipal prime ideals of k ramifying in K/k_1 are (for every ℓ dividing $\#H$ and every $\tau \in H\{\ell\}^*$):*

- (a) $\mathfrak{q}_{\tau, 1}, \mathfrak{q}_{\tau, 2}, \dots, \mathfrak{q}_{\tau, A_{\tau}}$, in the class of x_{τ} and such that, for any $i = 1, \dots, A_{\tau}$, the inertia group of every prime of K dividing $\mathfrak{q}_{\tau, i}$ is a conjugate of $\langle \tau^{\frac{o(\tau)}{\ell}} \rangle$;
- (b) $\mathfrak{q}_{\tau, A_{\tau}+1}, \mathfrak{q}_{\tau, A_{\tau}+2}$, in the class of $x_{\tau}^{B_{\tau}}$ and such that the inertia group of every prime of K dividing $\mathfrak{q}_{\tau, A_{\tau}+1}$ and $\mathfrak{q}_{\tau, A_{\tau}+2}$ is a conjugate of $\langle \tau \rangle$.

2. *We have*

$$\text{st}(K/k_1) = \prod_{\ell \mid \#H} \prod_{\tau \in H\{\ell\}^*} \iota(x_{\tau})^{A_{\tau} \frac{\ell-1}{2} \frac{\#H}{\ell} + B_{\tau}(o(\tau)-1) \frac{\#H}{o(\tau)}},$$

where $\iota : \text{Cl}(k) \rightarrow \text{Cl}(k_1)$ is induced by the inclusion $k \subseteq k_1$.

3. *K/k_1 satisfies $P(s)$.*

Proof. By Lemma 3.2 there exists a tame H -Galois extension \tilde{K} of k_1 , such that \tilde{K}/k is G -Galois, \tilde{K}/k_1 is ramified only at principal ideals and it satisfies $P(s)$.

Since k_1/k satisfies $P(s)$, by [8, Lemma 3.4] and Lemma 2.2, we have for every $\tau \in H^*$ that $W(k, E_{k, G, \tau}) = W(k, Z_{k_1/k, \mu, \tau})$, where $Z_{k_1/k, \mu, \tau}$ has been defined in [8]. This observation will allow us to argue as in [8, Lemma 3.11], but replacing $W(k, Z_{k_1/k, \mu, \tau})$ with $W(k, E_{k, G, \tau})$.

As in the proof of Lemma 3.2, we add all the v_{ρ_1, ρ_2} (defined in the proof of Lemma 3.2) to the set $\{u_1, \dots, u_T\}$ defined in [8], before Lemma 3.9. Now, for every prime number ℓ dividing $\#H$, for every $\tau \in H\{\ell\}^*$ and for every $i = 1, \dots, A_{\tau}$ (resp.

$i = A_{\tau+1}, A_{\tau+2}$) we choose prime ideals $\mathfrak{q}_{\tau,i}$ in the class of x_τ (resp. in the class of $x_\tau^{B_\tau}$). For any $i = 1, \dots, A_\tau + 2$, we also choose prime ideals $\mathfrak{Q}_{\tau,i}$ in k_1 dividing the $\mathfrak{q}_{\tau,i}$ and generators $g_{\mathfrak{Q}_{\tau,i}}$ of the units of the residue fields $\kappa_{\mathfrak{Q}_{\tau,i}}$. As in the proof of [8, Lemma 3.11], we can assume that the $\mathfrak{q}_{\tau,i}$ are unramified in $k_1(\zeta_s)/\mathbb{Q}$ and in \tilde{K}/k_1 .

For every prime number ℓ dividing $\#H$, for every $\tau \in H\{\ell\}^*$ and for every $i = 1, \dots, A_\tau + 2$, we define $\varphi_{\tau,i} : \kappa_{\mathfrak{Q}_{\tau,i}}^\times \rightarrow H$ as follows. If A_τ is odd, we set

$$\varphi_{\tau,i}(g_{\mathfrak{Q}_{\tau,i}}) = \begin{cases} \tau^{\frac{o(\tau)}{\ell}} & \text{if } i = 1, 2 \\ \tau^{-\frac{2o(\tau)}{\ell}} & \text{if } i = 3 \\ \tau^{(-1)^i \frac{o(\tau)}{\ell}} & \text{if } 4 \leq i \leq A_\tau \\ \tau^{(-1)^i} & \text{if } i = A_\tau + 1, A_\tau + 2. \end{cases}$$

If A_τ is even, we set

$$\varphi_{\tau,i}(g_{\mathfrak{Q}_{\tau,i}}) = \begin{cases} \tau^{(-1)^i \frac{o(\tau)}{\ell}} & \text{if } 1 \leq i \leq A_\tau \\ \tau^{(-1)^i} & \text{if } i = A_\tau + 1, A_\tau + 2. \end{cases}$$

As in the proof of [8, Lemma 3.11], using that $x_\tau \in W(k, E_{k,G,\tau})$, we can assume that the $\mathfrak{Q}_{\tau,i}$ and the $g_{\mathfrak{Q}_{\tau,i}}$ are such that the $\varphi_{\tau,i}$ are $D(k_1/k, \mathfrak{Q}_{\tau,i})$ -invariant. Hence, for $i = 1, \dots, A_\tau + 2$, we extend $\varphi_{\tau,i}$ to a \mathcal{G} -invariant homomorphism

$$\tilde{\varphi}_{\tau,i} : \text{ind}_{D(k_1/k, \mathfrak{Q}_{\tau,i})}^{\mathcal{G}} \kappa_{\mathfrak{Q}_{\tau,i}}^\times \cong \prod_{\delta \in \mathcal{G}/D(k_1/k, \mathfrak{Q}_{\tau,i})} \kappa_{\delta(\mathfrak{Q}_{\tau,i})}^\times \rightarrow H,$$

using the Frobenius reciprocity. We define $\varphi_0 : \prod_{\mathfrak{p}} \kappa_{\mathfrak{p}}^\times \rightarrow H$, setting

$$\begin{cases} \varphi_0|_{\kappa_{\delta(\mathfrak{Q}_{\tau,i})}^\times} = \tilde{\varphi}_{\tau,i} & \text{for } \ell | \#H, \tau \in H\{\ell\}^*, i = 1, \dots, A_\tau + 2 \text{ and } \delta \in \mathcal{G} \\ \varphi_0|_{\kappa_{\mathfrak{p}}^\times} = 1 & \text{for all the other primes.} \end{cases}$$

As in the proof of [8, Lemma 3.10], we can assume that all the elements u_j are in the kernel of φ_0 , so that we can extend φ_0 to a \mathcal{G} -invariant homomorphism $\varphi : C_{k_1} \rightarrow H$, whose kernel contains a congruence subgroup of C_{k_1} . Therefore taking the product

$$\varphi \cdot (\cdot, \tilde{K}/k_1) : C_{k_1} \rightarrow H,$$

we get a \mathcal{G} -invariant homomorphism whose kernel contains a congruence subgroup and which is surjective, by the assumptions on the ideals $\mathfrak{q}_{\tau,i}$.

By class field theory (see for example [8, Theorem 2.3 and Proposition 2.4]), we obtain a tame H -Galois extension K of k_1 , which is Galois over k . The extension K/k_1 satisfies $P(s)$, by the assumptions on the prime ideals $\mathfrak{q}_{\tau,i}$ and the fact that \tilde{K}/k_1 satisfies $P(s)$. As in the proof of Lemma 3.2, actually $\text{Gal}(K/k) \cong G$. All the requested properties hold, by construction, once more as in the proof of [8, Lemma 3.11]. \square

For any \mathcal{G} -Galois extension k_1 of k , we define $R_t(k_1, k, G) \subseteq \text{Cl}(k_1)$ as the set of those ideal classes of k_1 which are Steinitz classes of a tamely ramified H -Galois extension K/k_1 , such that K/k is G -Galois.

Lemma 3.4. *Let s be a multiple of $\#H$ and let k_1 be a tame \mathcal{G} -Galois extension of k satisfying $P(s)$. Then*

$$\prod_{\ell|\#H} \prod_{\tau \in H\{\ell\}^*} \iota(W(k, E_{k,G,\tau}))^{\frac{\ell-1}{2} \frac{\#H}{o(\tau)}} \subseteq R_t(k_1, k, G),$$

where $\iota : \text{Cl}(k) \rightarrow \text{Cl}(k_1)$ is induced by the inclusion $k \subseteq k_1$. Further any class in the left-hand side of the above inclusion is the Steinitz class of a tame H -Galois extension K/k_1 which satisfies $P(s)$ and such that K/k is G -Galois.

Proof. Let

$$x = \prod_{\ell|\#H} \prod_{\tau \in H\{\ell\}^*} x_\tau^{\frac{\ell-1}{2} \frac{\#H}{o(\tau)}} \in \prod_{\ell|\#H} \prod_{\tau \in H\{\ell\}^*} W(k, E_{k,G,\tau})^{\frac{\ell-1}{2} \frac{\#H}{o(\tau)}},$$

with $x_\tau \in W(k, E_{k,G,\tau})$. Let $o(x_\tau)$ be the order of $x_\tau \in \text{Cl}(k)$. Since any prime ℓ dividing $\#H$ is odd, for any $\tau \in H\{\ell\}^*$, using (1), we can find integers $A_\tau, B_\tau > 1$ such that

$$A_\tau \frac{\ell-1}{2} \frac{\#H}{\ell} + B_\tau(o(\tau)-1) \frac{\#H}{o(\tau)} \equiv \frac{\ell-1}{2} \frac{\#H}{o(\tau)} \pmod{o(x_\tau)}$$

and, in particular, we have

$$x_\tau^{A_\tau \frac{\ell-1}{2} \frac{\#H}{\ell} + B_\tau(o(\tau)-1) \frac{\#H}{o(\tau)}} = x_\tau^{\frac{\ell-1}{2} \frac{\#H}{o(\tau)}}.$$

Hence we conclude by Lemma 3.3, with A_τ and B_τ as above. \square

Theorem 3.5. *Let k be a number field and let \mathcal{G} be a finite group of odd order satisfying the second condition of Definition 2.17. Let H be an abelian group of odd order, let $\mu : \mathcal{G} \rightarrow \text{Aut}(H)$ be an action of \mathcal{G} on H and let $G = H \rtimes_\mu \mathcal{G}$. Then*

$$R_t(k, G) \supseteq R_t(k, \mathcal{G})^{\#H} \prod_{\ell|\#H} \prod_{\tau \in H\{\ell\}^*} W(k, E_{k,G,\tau})^{\frac{\ell-1}{2} \frac{\#G}{o(\tau)}}.$$

More precisely, for any class x in the right-hand side of the above inclusion and any positive integer s , there exists a tame G -Galois extension K/k with Steinitz class x and satisfying $P(s)$.

Proof. We will prove directly the last assertion of the theorem. Note that it suffices to prove it for s big enough. So let s be a positive integer which is a multiple of the order of H . Let

$$x \in R_t(k, \mathcal{G})^{\#H} \prod_{\ell|\#H} \prod_{\tau \in H\{\ell\}^*} W(k, E_{k,G,\tau})^{\frac{\ell-1}{2} \frac{\#G}{o(\tau)}}$$

and write $x = y^{\#H} z^{\#G}$ with $y \in R_t(k, \mathcal{G})$ and $z \in \prod_{\ell|\#H} \prod_{\tau \in H\{\ell\}^*} W(k, E_{k,G,\tau})^{\frac{\ell-1}{2} \frac{\#H}{o(\tau)}}$. By the hypothesis on \mathcal{G} , we can find a tame \mathcal{G} -Galois extension k_1/k with Steinitz class y and which satisfies $P(s)$.

Further, by Lemma 3.4, there exists an H -Galois extension K/k_1 , which satisfies $P(s)$, which is Galois over k , with Galois group G , and with $\text{st}(K/k_1) = \iota(z)$, where

$\iota : \text{Cl}(k) \rightarrow \text{Cl}(k_1)$ is induced by the inclusion $k \subseteq k_1$. Then, using a well-known formula relating the Steinitz classes in towers of extensions (see for example [10, Proposition I.1.2]), we get

$$\text{st}(K/k) = \text{st}(k_1/k)^{\#H} N_{k_1/k}(\text{st}(K/k_1)) = y^{\#H} N_{k_1/k}(\iota(z)) = y^{\#H} z^{\#G} = x,$$

where $N_{k_1/k} : \text{Cl}(k_1) \rightarrow \text{Cl}(k)$ is induced by the norm from k_1 to k . \square

Remark 3.6. The techniques described in this section can be extended to groups of even order, as in [7]. We have restricted our attention to groups of odd order only to have cleaner proofs and statements (as already noticed, there are groups of even order which are not very good). However the complications arising from extensions of even degree vanish if we assume that the class number of the base field k is odd.

4 A' -groups of odd order

In this section we find some slightly more explicit descriptions for the results of [8]. In particular we prove that the answer to Question 2.18 is affirmative for the so-called A' -groups of odd order, whose definition we now recall.

Definition 4.1. We define A' -groups inductively:

1. Finite abelian groups are A' -groups.
2. If \mathcal{G} is an A' -group and H is a finite abelian group of order prime to that of \mathcal{G} , then $H \rtimes_{\mu} \mathcal{G}$ is an A' -group, for any action $\mu : \mathcal{G} \rightarrow \text{Aut}(H)$ of \mathcal{G} on H .
3. If \mathcal{G}_1 and \mathcal{G}_2 are A' -groups, then $\mathcal{G}_1 \times \mathcal{G}_2$ is an A' -group.

Proposition 4.2. *Let \mathcal{G} be a very good group of odd order, let H be an abelian group of odd order prime to that of \mathcal{G} and let $\mu : \mathcal{G} \rightarrow \text{Aut}(H)$ be an action of \mathcal{G} on H . Then $G = H \rtimes_{\mu} \mathcal{G}$ is very good. In particular abelian groups are very good.*

Proof. Let $\pi : G \rightarrow G/H \cong \mathcal{G}$ be the projection. For any $\ell \nmid \# \mathcal{G}$ and any $\sigma \in G\{\ell\}$, there exists $\tilde{\sigma} \in \mathcal{G}\{\ell\}$ such that $\pi(\sigma) = \pi(\tilde{\sigma})$. Further, since σ and $\pi(\sigma)$ have the same order, it is straightforward to verify that

$$H_{k,G,\sigma} \subseteq H_{k,G/H,\pi(\sigma)} = H_{k,\mathcal{G},\tilde{\sigma}}.$$

Hence

$$E_{k,G,\sigma} \supseteq E_{k,\mathcal{G},\tilde{\sigma}}$$

and, by Lemma 2.6,

$$W(k, E_{k,G,\sigma}) \subseteq W(k, E_{k,\mathcal{G},\tilde{\sigma}}).$$

We also observe that for $\ell \nmid \# H$, $H\{\ell\} = G\{\ell\}$. Using Theorem 3.5 (but actually also [8, Theorem 3.19] would work in this case) and the hypothesis that \mathcal{G} is very good, we then have:

$$\begin{aligned} R_t(k, G) &\supseteq R_t(k, \mathcal{G})^{\#H} \prod_{\ell \nmid \# H} \prod_{\tau \in H\{\ell\}^*} W(k, E_{k,G,\tau})^{\frac{\ell-1}{2} \frac{\#G}{o(\tau)}} \\ &= \prod_{\ell \nmid \# \mathcal{G}} \prod_{\sigma \in \mathcal{G}\{\ell\}^*} W(k, E_{k,\mathcal{G},\sigma})^{\frac{\ell-1}{2} \frac{\#G}{o(\sigma)}} \prod_{\ell \nmid \# H} \prod_{\tau \in H\{\ell\}^*} W(k, E_{k,G,\tau})^{\frac{\ell-1}{2} \frac{\#G}{o(\tau)}} \\ &\supseteq \prod_{\ell \nmid \# G} \prod_{\sigma \in G\{\ell\}^*} W(k, E_{k,G,\sigma})^{\frac{\ell-1}{2} \frac{\#G}{o(\sigma)}} = \mathcal{W}(k, G). \end{aligned}$$

The opposite inclusion is given by Theorem 2.13. By Theorem 3.5 and the hypothesis that \mathcal{G} is very good, also the second condition of Definition 2.17 is satisfied by G . \square

Proposition 4.3. *Let $\mathcal{G}_1, \mathcal{G}_2$ be very good groups of odd order. Then $G = \mathcal{G}_1 \times \mathcal{G}_2$ is very good.*

Proof. Let ℓ be a prime number, let $\sigma_1 \in \mathcal{G}_1\{\ell\}$, $\sigma_2 \in \mathcal{G}_2\{\ell\}$ be not both trivial. Then $o(\sigma_1\sigma_2) = \max\{o(\sigma_1), o(\sigma_2)\} > 1$ and let us assume $o(\sigma_1\sigma_2) = o(\sigma_1)$. Clearly $N_G(\sigma_1\sigma_2) \subseteq N_G(\sigma_1)$ and, for every $\tau \in N_G(\sigma_1\sigma_2)$, we have

$$\varphi_{\sigma_1\sigma_2}(\tau) = \varphi_{\sigma_1}(\tau).$$

Therefore

$$H_{k,G,\sigma_1\sigma_2} \subseteq H_{k,G,\sigma_1},$$

i.e.

$$E_{k,G,\sigma_1\sigma_2} \supseteq E_{k,G,\sigma_1}.$$

Using Lemma 2.6 and Lemma 2.2, we conclude that

$$W(k, E_{k,G,\sigma_1\sigma_2})^{\frac{\ell-1}{2} \frac{\#G}{o(\sigma_1\sigma_2)}} \subseteq W(k, E_{k,G,\sigma_1})^{\frac{\ell-1}{2} \frac{\#G_1 \cdot \#G_2}{o(\sigma_1)}} = W(k, E_{k,\mathcal{G}_1,\sigma_1})^{\frac{\ell-1}{2} \frac{\#G_1}{o(\sigma_1)} \#G_2}$$

and an analogous result holds when $o(\sigma_1\sigma_2) = o(\sigma_2)$. Hence, using the hypothesis that \mathcal{G}_1 and \mathcal{G}_2 are very good groups of odd order,

$$\begin{aligned} \mathcal{W}(k, G) &= \prod_{\ell \mid \#G} \prod_{\sigma \in G\{\ell\}^*} W(k, E_{k,G,\sigma})^{\frac{\ell-1}{2} \frac{\#G}{o(\sigma)}} \\ &\subseteq \prod_{\ell \mid \#G_1} \prod_{\sigma_1 \in \mathcal{G}_1\{\ell\}^*} W(k, E_{k,\mathcal{G}_1,\sigma_1})^{\frac{\ell-1}{2} \frac{\#G_1}{o(\sigma_1)} \#G_2} \prod_{\ell \mid \#G_2} \prod_{\sigma_2 \in \mathcal{G}_2\{\ell\}^*} W(k, E_{k,\mathcal{G}_2,\sigma_2})^{\frac{\ell-1}{2} \frac{\#G_2}{o(\sigma_2)} \#G_1} \\ &= R_t(k, \mathcal{G}_1)^{\#G_2} R_t(k, \mathcal{G}_2)^{\#G_1}. \end{aligned}$$

In particular every class in $\mathcal{W}(k, G)$ is of the form $x_1^{\#G_2} x_2^{\#G_1}$, where $x_i \in R_t(k, \mathcal{G}_i)$ for $i = 1, 2$. Now let s be a positive integer: then, since \mathcal{G}_1 is very good, there exists a tame \mathcal{G}_1 -Galois extension k_1/k with Steinitz class x_1 and satisfying $P(s)$. Further let \tilde{s} be a multiple of s such that all the primes ramifying in k_1/k ramify also in $k(\zeta_{\tilde{s}})/k$. Now, since also \mathcal{G}_2 is very good, there exists a tame \mathcal{G}_2 -Galois extension k_2/k with Steinitz class x_2 and satisfying $P(\tilde{s})$. The compositum $K = k_1 k_2$ is a tame G -Galois extension of k , satisfying $P(s)$. Since k_1 and k_2 are linearly disjoint over k , we have $d(K/k) = d(k_1/k)^{\#G_2} d(k_2/k)^{\#G_1}$ and hence, by [8, Theorem 2.1],

$$\text{st}(K/k) = x_1^{\#G_2} x_2^{\#G_1},$$

since $\#G_1$ and $\#G_2$ are both odd.

Therefore $\mathcal{W}(k, G) \subseteq R_t(k, G)$ and the opposite inclusion is given by Theorem 2.13. Actually the above construction also proves the second property characterizing very good groups. \square

Putting things together, we obtain a refinement of [8, Theorem 3.23].

Theorem 4.4. *Every A' -group of odd order is very good.*

Proof. Obvious, by induction, using the above results. \square

5 Groups of order dividing ℓ^4

In this section, ℓ is an odd prime. We want to show that the answer to Question 2.18 is affirmative for all nonabelian groups of order dividing ℓ^4 (the abelian case is covered by Theorem 4.4). Further the same is true for all groups of order ℓ^n and exponent ℓ^{n-1} , for any positive integer n (these are actually the groups studied in [9]).

Lemma 5.1. *Let G be an ℓ -group and let $\tau \in G^*$. Set*

$$e_\tau = \frac{o(\tau)}{\#(N_G(\tau)/C_G(\tau))}.$$

Then $\ell | e_\tau$ and $E_{k,G,\tau} = k(\zeta_{e_\tau})$; in particular $\zeta_\ell \in E_{k,G,\tau}$.

Proof. Since the kernel of φ_τ is the centralizer $C_G(\tau)$, $\varphi_\tau(N_G(\tau))$ is the subgroup of order $\#(N_G(\tau)/C_G(\tau))$ of the ℓ -Sylow subgroup of the cyclic group $(\mathbb{Z}/o(\tau)\mathbb{Z})^\times$. This already gives $\ell | e_\tau$ and we also have

$$\varphi_\tau(N_G(\tau)) = 1 + \frac{o(\tau)}{\#(N_G(\tau)/C_G(\tau))} \mathbb{Z} \pmod{o(\tau)} = 1 + e_\tau \mathbb{Z} \pmod{o(\tau)}.$$

Therefore

$$H_{k,G,\tau} = \text{Gal}(k(\zeta_{o(\tau)})/k(\zeta_{e_\tau}))$$

and

$$E_{k,G,\tau} = k(\zeta_{e_\tau}) \supseteq k(\zeta_\ell).$$

□

Proposition 5.2 (Burnside). *A group of order ℓ^n , whose center has order ℓ^c , contains a normal abelian subgroup of order ℓ^ν where*

$$\nu \geq -\frac{1}{2} + \sqrt{2n + c^2 - c + \frac{1}{4}}.$$

In particular, for $n = 3, 4$ this becomes

$$\nu \geq n - 1.$$

Proof. This result is shown in [3, Section 4].

□

We shall use the above proposition for $n = 3, 4$. For these values of n the result actually follows quite easily using standard arguments of the theory of ℓ -groups. From now on we will use the notation $C(n)$ to denote a cyclic group of order n , where n is a positive integer.

Lemma 5.3. *Let G be a group of exponent ℓ and order ℓ^n , where $n = 3, 4$. Then G is very good and in particular*

$$R_t(k, G) = W(k, \ell)^{\frac{\ell-1}{2}\ell^{n-1}}.$$

Proof. By Proposition 5.2, there is an exact sequence

$$1 \rightarrow C(\ell)^{n-1} \rightarrow G \rightarrow C(\ell) \rightarrow 1,$$

which splits, since the exponent of G is ℓ .

Using Lemma 5.1, we get $\mathcal{W}(k, G) = W(k, \ell)^{\frac{\ell-1}{2}\ell^{n-1}}$ and the proof of the equality $R_t(k, G) = \mathcal{W}(k, G)$ is straightforward, using Theorem 2.13 and Theorem 3.5 (which we can apply with $\mathcal{G} = C(\ell)$ and $H = C(\ell)^{n-1}$, since $C(\ell)$ is very good by Theorem 4.4).

Since in particular every $x \in R_t(k, G)$ belongs to the right-hand side of the inclusion of Theorem 3.5, it follows by Theorem 3.5 that G satisfies the second condition of Definition 2.17. \square

The above result for $n = 3$ is actually proved in [1, Corollaire 1.2]. The following result slightly improves [9, Theorem 3.8].

Proposition 5.4. *Let G be a nonabelian group of order ℓ^n and exponent ℓ^{n-1} , where $n > 2$ is an integer. Then G is very good and*

$$R_t(k, G) = W(k, \ell^{n-2})^{\frac{\ell-1}{2}\ell}.$$

Proof. As it is well known (and easily verified), G can be written as

$$G = \langle \sigma, \tau : \sigma^\ell = \tau^{\ell^{n-1}} = 1, \sigma\tau\sigma^{-1} = \tau^{1+\ell^{n-2}} \rangle.$$

Clearly $\langle \tau^\ell \rangle$ equals the center of G , which has therefore order ℓ^{n-2} . Let $\rho = \tau^a \sigma^b \in G$, with $\sigma^b \neq 1$ (resp. $\sigma^b = 1$), then $\tau^a \sigma^b$ (resp. τ) is an element of the centralizer of $\tau^a \sigma^b$ which is not in the center of G . Thus, for any element $\rho \in G$, the order of $C_G(\rho)$ is strictly larger than that of the center of G and hence $\#C_G(\tau)$ is a multiple of ℓ^{n-1} . Therefore $\#(N_G(\tau)/C_G(\tau))$ divides ℓ and $\frac{o(\rho)}{\ell}|e_\rho$, i.e. $k(\zeta_{o(\rho)/\ell}) \subseteq E_{k,G,\rho}$, by Lemma 5.1.

Hence, using Lemma 2.6 and Lemma 2.7, if $\ell^2|o(\rho)$, then

$$W(k, E_{k,G,\rho})^{\frac{\ell-1}{2}\frac{\ell^n}{o(\rho)}} \subseteq W(k, o(\rho)/\ell)^{\frac{\ell-1}{2}\frac{\ell^n}{o(\rho)}} \subseteq W(k, \ell^{n-2})^{\frac{\ell-1}{2}\ell}.$$

If $\rho \neq 1$ and $\ell^2 \nmid o(\rho)$, i.e. $o(\rho) = \ell$, then by Lemma 5.1 we must have $E_{k,G,\rho} = k(\zeta_\ell)$. Hence, again using Lemma 2.6 and Lemma 2.7,

$$W(k, E_{k,G,\rho})^{\frac{\ell-1}{2}\frac{\ell^n}{o(\rho)}} = W(k, \ell)^{\frac{\ell-1}{2}\ell^{n-1}} \subseteq W(k, \ell^{n-1})^{\frac{\ell-1}{2}\ell} \subseteq W(k, \ell^{n-2})^{\frac{\ell-1}{2}\ell}.$$

Further, we have $N_G(\tau) = G$ and $C_G(\tau) = \langle \tau \rangle$ and therefore, by Lemma 5.1,

$$W(k, E_{k,G,\tau})^{\frac{\ell-1}{2}\frac{\ell^n}{o(\tau)}} = W(k, \ell^{n-2})^{\frac{\ell-1}{2}\ell}.$$

Therefore

$$\mathcal{W}(k, G) = \prod_{\rho \in G^*} W(k, E_{k,G,\rho})^{\frac{\ell-1}{2}\frac{\ell^n}{o(\rho)}} = W(k, E_{k,G,\tau})^{\frac{\ell-1}{2}\ell}.$$

We easily conclude by Theorems 2.13, 3.5 and 4.4, as in the proof of Lemma 5.3. \square

Lemma 5.5. *Let G be a nonabelian group of order ℓ^4 and exponent ℓ^2 . Let $\tau \in G$ be of order ℓ^2 and such that $\#(N_G(\tau)/C_G(\tau))$ is maximal. Then $\mathcal{W}(k, G) = W(k, E_{k,G,\tau})^{\frac{\ell-1}{2}\ell^2}$.*

Proof. For any $\sigma \in G$ of order ℓ , using Lemma 5.1, Lemma 2.7 and Lemma 2.6, we have

$$W(k, E_{k,G,\sigma})^{\frac{\ell-1}{2} \frac{\ell^4}{o(\sigma)}} = W(k, \ell)^{\frac{\ell-1}{2} \ell^3} \subseteq W(k, \ell^2)^{\frac{\ell-1}{2} \ell^2} \subseteq W(k, E_{k,G,\tau})^{\frac{\ell-1}{2} \ell^2}.$$

Further for any $\sigma \in G$ of order ℓ^2 we have $\#(N_G(\sigma)/C_G(\sigma)) \leq \#(N_G(\tau)/C_G(\tau))$, i.e., by Lemma 5.1, $E_{k,G,\sigma} \supseteq E_{k,G,\tau}$, and hence, by Lemma 2.6,

$$W(k, E_{k,G,\sigma}) \subseteq W(k, E_{k,G,\tau}).$$

Therefore

$$\mathcal{W}(k, G) = \prod_{\rho \in G^*} W(k, E_{k,G,\rho})^{\frac{\ell-1}{2} \frac{\ell^4}{o(\rho)}} = W(k, E_{k,G,\tau})^{\frac{\ell-1}{2} \ell^2}.$$

□

Lemma 5.6. *Let G be a (nonabelian) group of order ℓ^4 and exponent ℓ^2 . Then there exists a normal abelian subgroup H of order ℓ^3 and an element $\tau \in G$ of order ℓ^2 maximizing $\#(N_G(\tau)/C_G(\tau))$, such that we have one of the following possibilities:*

1. $\tau \in H$ and $G \cong H \rtimes C(\ell)$.
2. $G \cong \langle \tau \rangle \rtimes C(\ell^2)$.
3. $\tau \notin H$ and there exists $\sigma_1 \in N_G(\tau) \setminus \langle \tau \rangle$ of order ℓ , which acts trivially (resp. nontrivially) on τ if $N_G(\tau) = C_G(\tau)$ (resp. if $N_G(\tau) \neq C_G(\tau)$).

Proof. Let $\sigma \in G$ be an element of order ℓ^2 , which maximizes $\#(N_G(\sigma)/C_G(\sigma))$; since, by Lemma 5.1, ℓ divides

$$e_\sigma = \frac{o(\sigma)}{\#(N_G(\sigma)/C_G(\sigma))} = \frac{\ell^2}{\#(N_G(\sigma)/C_G(\sigma))},$$

we have that $\#(N_G(\sigma)/C_G(\sigma))$ divides ℓ . We will study separately the cases $\#C_G(\sigma) \geq \ell^3$ and $\#C_G(\sigma) = \ell^2$.

- If $\#C_G(\sigma) \geq \ell^3$, then we set H to be a subgroup of order ℓ^3 of $C_G(\sigma)$ containing σ . Clearly H is abelian and normal, being of index ℓ , and we have an exact sequence

$$1 \rightarrow H \rightarrow G \rightarrow C(\ell) \rightarrow 1. \quad (3)$$

There are three cases, corresponding to the three possibilities in the statement of the lemma.

1. Sequence (3) splits. Then we set $\tau = \sigma \in H$ and we have $G \cong H \rtimes C(\ell)$.
2. Sequence (3) does not split and $\#(N_G(\sigma)/C_G(\sigma)) = \ell$. In this case $N_G(\sigma) = G$, $C_G(\sigma) = H$ and we consider an element $\rho \in G \setminus H$. If $\#\langle \sigma, \rho \rangle = \ell^3$, then $\langle \sigma, \rho \rangle \cong C(\ell^2) \rtimes C(\ell)$ and there would exist an element of order ℓ in $N_G(\sigma) \setminus C_G(\sigma) = G \setminus H$, contradicting the assumption that (3) does not split. Therefore $\langle \sigma, \rho \rangle = G$ and, setting $\tau = \sigma$, we get $G = \langle \tau \rangle \rtimes \langle \rho \rangle$.

3. Sequence (3) does not split and $\#(N_G(\sigma)/C_G(\sigma)) = 1$. In this case, by the assumption of maximality, an analogous condition holds for every element of order ℓ^2 . So we can take τ to be any element not in H , since it must be of order ℓ^2 because of the nonsplitting of (3). Further let \tilde{H} be a subgroup of order ℓ^3 of $N_G(\tau) = C_G(\tau)$ (which has order at least ℓ^3 , since τ is of order ℓ^2) and containing τ . Clearly \tilde{H} is abelian and we can find an element σ_1 of order ℓ in $\tilde{H} \setminus \langle \tau \rangle \subseteq N_G(\tau) \setminus \langle \tau \rangle$. In particular σ_1 acts trivially on τ .
- If $\#C_G(\sigma) = \ell^2$, i.e. $C_G(\sigma) = \langle \sigma \rangle$, then $\#N_G(\sigma) = \ell^3$, since it must be at least ℓ^3 , being strictly larger than $\langle \sigma \rangle$, and $N_G(\sigma)$ cannot be G , since $\#(N_G(\sigma)/C_G(\sigma))$ divides ℓ . By Proposition 5.2 there exists an abelian subgroup $H < G$ of order ℓ^3 . Clearly $\sigma \notin H$, since $\#C_G(\sigma) = \ell^2$. Further $N_G(\sigma)$ is nonabelian of order ℓ^3 and exponent ℓ^2 , so there exists $\sigma_1 \in N_G(\sigma) \setminus \langle \sigma \rangle$ of order ℓ , acting nontrivially on σ . Hence we are again in case 3, taking $\tau = \sigma$.

□

Lemma 5.7. *Let G be of the first or second type described in Lemma 5.6. Then G is very good and*

$$R_t(k, G) = W(k, E_{k,G,\tau})^{\frac{\ell-1}{2}\ell^2},$$

where $\tau \in G$ is as in Lemma 5.6.

Proof. By Lemma 5.5, we have $\mathcal{W}(k, G) = W(k, E_{k,G,\tau})^{\frac{\ell-1}{2}\ell^2}$. By Theorem 3.5, with $\mathcal{G} = C(\ell)$ or $C(\ell^2)$ (note that both are very good groups by Theorem 4.4), we obtain

$$\mathcal{W}(k, G) = W(k, E_{k,G,\tau})^{\frac{\ell-1}{2}\ell^2} \subseteq R_t(k, G).$$

The opposite inclusion is given by Theorem 2.13. The second condition of the definition of very good groups is immediate, as in the proof of Lemma 5.3. □

Lemma 5.8. *Let G be of the third type described in Lemma 5.6. Then G is very good and*

$$R_t(k, G) = W(k, E_{k,G,\tau})^{\frac{\ell-1}{2}\ell^2},$$

where $\tau \in G$ is as in Lemma 5.6.

Proof. By hypothesis there exists a normal abelian subgroup H of G of order ℓ^3 and an element $\tau \in G \setminus H$ of order ℓ^2 maximizing $\#(N_G(\tau)/C_G(\tau))$. We can also find an element $\sigma_1 \in N_G(\tau) \setminus \langle \tau \rangle$ of order ℓ and acting trivially on τ if and only if $N_G(\tau) = C_G(\tau)$. Let \mathcal{G} be the subgroup of G generated by σ_1 and τ , which must be of the form $C(\ell^2) \rtimes C(\ell)$, possibly with trivial action. Clearly there exists an integer a such that $\sigma_1 \tau \sigma_1^{-1} = \tau^{1+a\ell}$ (since the order of the conjugation divides ℓ). Since $\tau \notin H$, we have that τH generates G/H ; in particular, $\sigma_1 = \sigma \tau^b$, for some $\sigma \in H^*$ (not necessarily of order ℓ) and $b \in \mathbb{N}$. We also have

$$\sigma \tau \sigma^{-1} = \tau^{1+a\ell}.$$

For later use, we note that, since \mathcal{G} has order ℓ^3 and exponent ℓ^2 , there must exist $c \in \{0, 1, \dots, \ell-1\}$ such that $\sigma^\ell = \tau^{c\ell}$ (an easy calculation shows that $c = -b$, but we won't need it), so that we have

$$\mathcal{G} = \langle \sigma, \tau : \tau^{\ell^2} = \sigma^\ell \tau^{-c\ell} = 1, \sigma \tau \sigma^{-1} = \tau^{1+a\ell} \rangle.$$

We now consider the (abstract) group $\tilde{\mathcal{G}}$, generated by $\tilde{\sigma}$ and $\tilde{\tau}$, satisfying the same relations as σ and τ in \mathcal{G} . We also consider the element $\tilde{\sigma}_1 \in \tilde{\mathcal{G}}$, corresponding to $\sigma_1 \in \mathcal{G}$.

We define an action $\mu : \tilde{\mathcal{G}} \rightarrow \text{Aut}(H)$ by setting, for any $h \in H$,

$$\begin{cases} \mu(\tilde{\tau})(h) = \tau h \tau^{-1} \\ \mu(\tilde{\sigma})(h) = \sigma h \sigma^{-1} = h. \end{cases}$$

We consider the semidirect product

$$\tilde{G} = H \rtimes_{\mu} \tilde{\mathcal{G}}.$$

For every couple h_1, h_2 of elements of H , we want to define a surjective homomorphism $\pi : \tilde{G} \rightarrow G$, such that $\pi(h_1 \tilde{\tau})$ and $\pi(h_2 \tilde{\tau})$ are both of order ℓ^2 and $\ker(\pi) \cap H$ is trivial. There are two cases:

1. For every $h \in H$, $h\tau$ is of order ℓ^2 .

In this case we define $\pi : \tilde{G} \rightarrow G$ by removing tildes. Then π is clearly a surjective homomorphism, $\pi(h\tilde{\tau}) = h\tau$ has order ℓ^2 for any $h \in H$ and $\ker(\pi)$ has trivial intersection with H .

2. There exists an element $h_0 \in H$ such that $h_0\tau$ is of order ℓ .

Note that in this case, if for example $h_1 = h_0$, we cannot define π simply by removing tildes because $\pi(h_0 \tilde{\tau}) = h_0\tau$ would have order ℓ . Then we proceed as follows: by assumption,

$$(h_0\tau)^\ell = \left(\prod_{i=0}^{\ell-1} \tau^i h_0 \tau^{-i} \right) \tau^\ell = 1, \quad \text{i.e.} \quad \prod_{i=0}^{\ell-1} (\tau^i h_0 \tau^{-i}) = \tau^{-\ell}.$$

It follows that, for any $j \in \mathbb{Z}$,

$$(h_0^j \tau)^\ell = \left(\prod_{i=1}^{\ell-1} \tau^i h_0^j \tau^{-i} \right) \tau^\ell = \left(\prod_{i=1}^{\ell-1} \tau^i h_0 \tau^{-i} \right)^j \tau^\ell = \tau^{\ell(1-j)}.$$

Now, for any $j \in \mathbb{Z}$, we want to define a homomorphism $\pi_j : \tilde{G} \rightarrow G$ by setting

$$\begin{cases} \pi_j(\tilde{\tau}) = h_0^j \tau \\ \pi_j(\tilde{\sigma}) = \sigma^{1-j} \\ \pi_j(h) = h, \quad \forall h \in H. \end{cases}$$

We have to verify that the definition is compatible with the relations of \tilde{G} :

$$\begin{aligned}
\pi_j(\tilde{\sigma})\pi_j(\tilde{\tau})\pi_j(\tilde{\sigma}^{-1}) &= \sigma^{1-j}h_0^j\tau\sigma^{-(1-j)} = h_0^j\sigma^{1-j}\tau\sigma^{-(1-j)} \\
&= h_0^j\tau^{1+a\ell(1-j)} = h_0^j\tau(h_0^j\tau)^{a\ell} = (h_0^j\tau)^{1+a\ell} \\
&= \pi_j(\tilde{\tau}^{1+a\ell}); \\
\pi_j(\tilde{\tau})\pi_j(h)\pi_j(\tilde{\tau}^{-1}) &= h_0^j\tau h\tau^{-1}h_0^{-j} = \tau h\tau^{-1} \\
&= \pi_j(\tau h\tau^{-1}); \\
\pi_j(\tilde{\sigma})\pi_j(h)\pi_j(\tilde{\sigma}^{-1}) &= \sigma^{1-j}h\sigma^{-(1-j)} = h \\
&= \pi_j(h); \\
\pi_j(\tilde{\sigma})^\ell &= \sigma^{(1-j)\ell} = \tau^{c\ell(1-j)} = (h_0^j\tau)^{c\ell} \\
&= \pi_j(\tilde{\tau})^{c\ell}; \\
\pi_j(\tilde{\tau})^{\ell^2} &= (h_0^j\tau)^{\ell^2} = \tau^{\ell^2(1-j)} = 1 \\
&= \pi_j(1).
\end{aligned}$$

So, for any $j \in \mathbb{Z}$, $\pi_j : \tilde{G} \rightarrow G$ is indeed a homomorphism, which is clearly surjective and whose kernel has trivial intersection with H . Now let h_1, h_2 be two elements in H . We want to choose j such that $\pi_j(h_1\tilde{\tau})$ and $\pi_j(h_2\tilde{\tau})$ are both of order ℓ^2 . For $i = 1, 2$, we can find $h'_i \in H$ such that $(h_i\tilde{\tau})^\ell = h'_i\tilde{\tau}^\ell$. Then, for $i = 1, 2$,

$$\pi_j(h'_i\tilde{\tau}^\ell) = h'_i(h_0^j\tau)^\ell = h'_i\tau^{\ell(1-j)}.$$

Since $h'_i\tau^{\ell(1-j_1)} \neq h'_i\tau^{\ell(1-j_2)}$ if $j_1 \not\equiv j_2 \pmod{\ell}$, we have at least $\ell - 1 \geq 2$ choices for j such that $\pi_j(h'_i\tilde{\tau}^\ell) \neq 1$. Among those choices, at least $\ell - 2 \geq 1$ give also $\pi_j(h'_2\tilde{\tau}^\ell) \neq 1$.

Hence, in both cases, for every couple h_1, h_2 of elements of H , we have defined a projection $\pi : \tilde{G} \rightarrow G$, such that $\pi(h_1\tilde{\tau})$ and $\pi(h_2\tilde{\tau})$ are of order ℓ^2 and $\ker(\pi)$ has trivial intersection with H . With this in mind, we start constructing the extensions needed to prove the lemma.

Let k be a number field, let $x \in W(k, E_{k,G,\tau})$ and let s be a positive multiple of ℓ^3 (this hypothesis will be used later to apply Lemma 3.3). Since ℓ is an odd prime, there exist integers $A, B > 1$ such that

$$\ell A + 2(\ell + 1)B \equiv 1 \pmod{o(x)}$$

and, in particular, we have

$$x^{\ell A + 2(\ell + 1)B} = x.$$

By Lemma 3.2 there exists a tame $C(\ell)$ -Galois extension \tilde{k}_0/k ramified only at principal ideals and satisfying $P(s)$. Since $\tilde{\mathcal{G}} = \langle \tilde{\tau} \rangle \rtimes \langle \tilde{\sigma}_1 \rangle$, possibly with trivial action, and thanks to our assumption on σ_1 , we have $x \in W(k, E_{k,G,\tau}) = W(k, E_{k,\tilde{\mathcal{G}},\tilde{\tau}})$. So we can apply Lemma 3.3 (with $x_{\tilde{\tau}} = x$, $x_{\tilde{\rho}} = 1$ for every $\tilde{\rho} \in \langle \tilde{\tau} \rangle^* \setminus \{\tilde{\tau}\}$, $A_{\tilde{\tau}} = 0$ and $B_{\tilde{\tau}} = B$) and construct a tame $C(\ell^2)$ -Galois extension \tilde{k}_1/\tilde{k}_0 , such that \tilde{k}_1/k is $\tilde{\mathcal{G}}$ -Galois and it satisfies the following conditions.

- The only nonprincipal prime ideals of k ramifying in \tilde{k}_1/\tilde{k}_0 are $\mathfrak{p}_1, \mathfrak{p}_2$ in the class of x^B and the inertia group of every prime of \tilde{k}_1 dividing these \mathfrak{p}_i is $\langle \tilde{\tau} \rangle$ in $\tilde{\mathcal{G}} = \text{Gal}(\tilde{k}_1/k)$ ($\langle \tilde{\tau} \rangle$ is invariant by conjugation, since it is normal in $\tilde{\mathcal{G}}$);

- \tilde{k}_1/\tilde{k}_0 satisfies $P(s)$.

Now we want to construct an H -Galois extension \tilde{K}/\tilde{k}_1 . By Lemma 2.6 and Lemma 5.1, we have $x \in W(k, E_{k,G,\tau}) \subseteq W(k, \ell) = W(k, E_{k,\tilde{G},\rho})$ for every $\rho \in H$ of order ℓ . Hence again we can use Lemma 3.3 (with $x_{\rho_0} = x$, for a certain $\rho_0 \in H^*$ of order ℓ , $x_\rho = 1$ for every $\rho \in H^* \setminus \{\rho_0\}$, $A_{\rho_0} = A$ and $B_{\rho_0} = 0$) to find a tame H -Galois extension \tilde{K}/\tilde{k}_1 , such that \tilde{K}/k is \tilde{G} -Galois and satisfies the following conditions.

- The only nonprincipal prime ideals of k ramifying in \tilde{K}/\tilde{k}_1 are $\mathfrak{p}_3, \dots, \mathfrak{p}_{A+2}$ in the class of x and the inertia group of every prime of \tilde{K} dividing these \mathfrak{p}_i is generated by a conjugate of ρ_0 in $\tilde{G} = \text{Gal}(\tilde{K}/k)$.
- \tilde{K}/\tilde{k}_1 satisfies $P(s)$ (in particular it follows that $\{\mathfrak{p}_1, \mathfrak{p}_2\} \cap \{\mathfrak{p}_3, \dots, \mathfrak{p}_{A+2}\} = \emptyset$).

Let us consider two prime ideals $\tilde{\mathfrak{P}}_1$ and $\tilde{\mathfrak{P}}_2$ of \tilde{K} dividing \mathfrak{p}_1 and \mathfrak{p}_2 respectively. Their inertia groups in the extension \tilde{K}/k must be generated by elements of the form $h_i \tilde{\tau}$ for some $h_i \in H$, $i = 1, 2$. We consider a projection $\pi : \tilde{G} \rightarrow G$ for which $\pi(h_1 \tilde{\tau})$ and $\pi(h_2 \tilde{\tau})$ are both of order ℓ^2 and such that $\ker(\pi)$ has trivial intersection with H . We call K the fixed field of $\ker(\pi)$. By construction the ramification index of \mathfrak{p}_1 and \mathfrak{p}_2 in K/k is ℓ^2 . Further the inertia group of the primes of \tilde{K} dividing $\mathfrak{p}_3, \dots, \mathfrak{p}_{A+2}$ lies in H , which has trivial intersection with $\ker(\pi)$. Therefore $\mathfrak{p}_3, \dots, \mathfrak{p}_{A+2}$ ramify in K/k , with ramification index ℓ and all the other ramifying primes are principal. Hence the discriminant of K/k is

$$d(K/k) = (\mathfrak{p}_1 \mathfrak{p}_2)^{(\ell^2-1)\ell^2} \prod_{i=3}^{A+2} \mathfrak{p}_i^{(\ell-1)\ell^3} I^2,$$

where I is a principal ideal. Hence, by [8, Theorem 2.1], the Steinitz class is

$$\text{st}(K/k) = x^{B(\ell^2-1)\ell^2 + A\frac{\ell-1}{2}\ell^3} = x^{\frac{\ell-1}{2}\ell^2(2(\ell+1)B + \ell A)} = x^{\frac{\ell-1}{2}\ell^2}.$$

Hence, recalling also Lemma 5.5, we have

$$\mathcal{W}(k, G) = W(k, E_{k,G,\tau})^{\frac{\ell-1}{2}\ell^2} \subseteq R_t(k, G),$$

We conclude, by Theorem 2.13, that

$$R_t(k, G) = \mathcal{W}(k, G).$$

As in the proof of Lemma 5.3, the second condition of Definition 2.17 holds, since the extensions we have constructed all satisfy $P(s')$ for every s' dividing s . \square

Theorem 5.9. *Let ℓ be an odd prime. Then every group of order dividing ℓ^4 is very good. In particular*

$$R_t(k, G) = \mathcal{W}(k, G).$$

Proof. If G is abelian, the theorem is a consequence of Theorem 4.4. So suppose that G is nonabelian. If G is of exponent ℓ , then the theorem follows from Lemma 5.3. If G is of order ℓ^n and exponent ℓ^{n-1} , for $n = 3, 4$, then the result is given by Proposition 5.4. We are therefore left with the case where G has order ℓ^4 and exponent ℓ^2 and we conclude by Lemma 5.6, Lemma 5.7 and Lemma 5.8. \square

Acknowledgements

We wish to thank Maurizio Monge for sharing with us some of his insights in the theory of ℓ -groups. Further we wish to thank the institutions which are supporting our research, i.e. the Université de Limoges and the Scuola Normale Superiore of Pisa.

References

- [1] C. BRUCHE, *Classes de Steinitz d'extensions non abéliennes de degré p^3* , Acta Arith., 137 (2009), pp. 177–191.
- [2] C. BRUCHE AND B. SODAÏGUI, *On realizable Galois module classes and Steinitz classes of nonabelian extensions*, J. Number Theory, 128 (2008), pp. 954–978.
- [3] W. BURNSIDE, *On some properties of groups whose orders are powers of primes*, Lond. M. S. Proc. (2), 11 (1913), pp. 225–245.
- [4] N. P. BYOTT, C. GREITHER, AND B. SODAÏGUI, *Classes réalisables d'extensions non abéliennes*, J. Reine Angew. Math., 601 (2006), pp. 1–27.
- [5] J. E. CARTER, *Steinitz classes of a nonabelian extension of degree p^3* , Colloq. Math., 71 (1996), pp. 297–303.
- [6] J. E. CARTER AND B. SODAÏGUI, *Classes de Steinitz d'extensions quaternioniennes généralisées de degré $4p^r$* , J. Lond. Math. Soc. (2), 76 (2007), pp. 331–344.
- [7] A. COBBE, *Steinitz classes of some abelian and nonabelian extensions of even degree*, J. Théor. Nombres Bordeaux, 22 (2010), pp. 607–628.
- [8] —, *Steinitz classes of tamely ramified galois extensions of algebraic number fields*, Journal of Number Theory, 130 (2010), pp. 1129 – 1154.
- [9] —, *Steinitz classes of tamely ramified nonabelian extensions of odd prime power order*, Acta Arith., 149 (2011), pp. 347–359.
- [10] L. P. ENDO, *Steinitz classes of tamely ramified Galois extensions of algebraic number fields*, PhD thesis, University of Illinois at Urbana-Champaign, 1975.
- [11] M. GODIN AND B. SODAÏGUI, *Classes de Steinitz d'extensions à groupe de Galois A_4* , J. Théor. Nombres Bordeaux, 14 (2002), pp. 241–248.
- [12] —, *Module structure of rings of integers in octahedral extensions*, Acta Arith., 109 (2003), pp. 321–327.
- [13] R. MASSY AND B. SODAÏGUI, *Classes de Steinitz et extensions quaternioniennes*, Proyecciones, 16 (1997), pp. 1–13.
- [14] L. R. MCCULLOH, *Galois module structure of abelian extensions*, J. Reine Angew. Math., 375/376 (1987), pp. 259–306.
- [15] —, *On realizable classes for nonabelian extensions (unpublished)*

- [16] —, *Informal report: Galois module to Steinitz classes (unpublished)*
- [17] A. N. PARSHIN AND I. R. SHAFAREVICH, eds., *Number theory. II*, vol. 62 of Encyclopaedia of Mathematical Sciences, Springer-Verlag, Berlin, 1992.
- [18] F. SBEITY AND B. SODAÏGUI, *Classes de Steinitz d'extensions non abéliennes à groupe de Galois d'ordre 16 ou extraspecial d'ordre 32 et problème de plongement*, Int. J. Number Theory, 6 (2010), pp. 1769–1783.
- [19] J.-P. SERRE, *Local fields*, vol. 67 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1979.
- [20] B. SODAÏGUI, *Classes de Steinitz d'extensions galoisiennes relatives de degré une puissance de 2 et problème de plongement*, Illinois J. Math., 43 (1999), pp. 47–60.
- [21] —, *Relative Galois module structure and Steinitz classes of dihedral extensions of degree 8*, J. Algebra, 223 (2000), pp. 367–378.
- [22] E. SOVERCHIA, *Steinitz classes of metacyclic extensions*, J. London Math. Soc. (2), 66 (2002), pp. 61–72.
- [23] THE PARI GROUP, *PARI/GP, version 2.5.0*, Bordeaux, 2011, available from <http://pari.math.u-bordeaux.fr/>.

Alessandro Cobbe
 Scuola Normale Superiore
 piazza Cavalieri, 7
 56126 Pisa
 Italy
 a.cobbe@sns.it

Luca Caputo
 Faculté de Sciences et Techniques
 123 Avenue Albert Thomas
 87060 Limoges
 France
 luca.caputo@unilim.fr